CLAIMS

1. A method of limiting a service to members of a group who are registered with a membership authority, wherein:

a provider of said service encrypts data based on encryption parameters comprising public data provided by the membership authority and an encryption key string, and the encrypted data is provided to a party;

to receive the service, said party must decrypt the encrypted data for which purpose it must obtain a decryption key from the membership authority;

the membership authority provides the decryption key to the party only if the latter is registered with the authority as a member of said group, the authority generating the decryption key in dependence on said encryption key string and private data related to said public data .

2. A method according to claim 1, wherein the encryption key string is created in whole or in part by the service provider..

3. A method according to claim 1, wherein the encryption key string is created in whole or in part by the service provider upon receipt of a service request from said party, the requesting party receiving the encryption key string from the service provider and providing it to the membership authority, and the membership authority only returning the decryption key after confirming that the party is a registered group member.

4. A method according to claim 1, wherein said party creates the encryption key string and provides it to the service provider when requesting said service, the party obtaining the decryption key from the membership authority either before or after requesting said service from the service provider.

5. A method according to claim 4, wherein the encryption key string is formed using information about at least one of said party and the membership authority, this information

being used by the service provider in the process of determining whether to provide said service to said party.

6. A method according to claim 1, wherein the encryption and decryption keys are created by the membership authority and provided to said party on the latter becoming a registered member of said group.

7. A method according to claim 6, wherein the encryption key string is formed using information about at least one of said party and the membership authority, this information being used by the service provider in the process of determining whether to provide said service to said party.

8. A method according to claim 1, wherein the data that is encrypted by the service provider is a data component of the service, said party only being able to decrypt and use this data component if it is a registered member of said group.

9. A method according to claim 8, wherein the data component comprises at least one of software and digital media content.

10. A method according to claim 1, wherein the data that is encrypted by the service provider is arbitrary data, said party being required to decrypt and return this data as evidence of its membership of said group before the service provider provides said service to the party.

11. A method according to claim 1, wherein in order to obtain the decryption key from the membership authority, said party proves its identity to the membership authority by using a secure entity authentication protocol.

12. A method according to claim 11, wherein the entity authentication protocol uses a secret that is securely stored in a trusted computing platform the integrity of which is checked by the membership authority before it accepts the proof of identity provided by said party.

13. A method according to claim 1, wherein the membership authority checks that said party is a registered member of said group before generating said decryption key.

14. A method according to claim 1, wherein the cryptographic processes involving said encryption and decryption keys are identifier-based cryptographic processes utilising quadratic residuosity.

15. A method according to claim 1, wherein the cryptographic processes involving the said encryption and decryption keys are identifier-based cryptographic processes utilising Weil or Tate pairings.

16. A method according to claim 1, wherein multiple groups are registered with the membership authority with each group having respective associated said public and private data, the service provider encrypting the data to be provided to said party using the public data of the group to which the service provider requires that party to belong in order to receive the service, this group being identified to the membership authority to enable it to check the party's membership of that group and to provide the appropriate decryption key by using the private data associated with that group when generating the decryption key.

17. A method according to claim 1, wherein multiple groups are registered with the membership authority and the same said public and private data is used in respect of all groups, the service provider encrypting the data to be provided to the requesting party using an encryption key string formed using at least an identifier of the group to which the service provider requires that party to belong in order to receive the service, the membership authority determining from the encryption key string the group in respect of which it is to check the membership of said party before it provides the decryption key to that party.

18. A method according to claim 1, wherein the service provider provides the service to members of said group as a result of a prior arrangement with the group representatives.

19. A method according to claim 1, wherein the service provider provides the service to parties meeting a particular condition, the service provider providing the service to members of said group after having determined that said condition is a predetermined membership requirement of said group.

20. A method of enabling a service provider to limit service access to parties meeting multiple conditions each of which corresponds to a predetermined membership requirement of a different group whose members are registered with an associated membership authority, wherein the method of claim 1 is applied in to check each condition using the said public and private data appropriate for the group that has the corresponding membership requirement.

21. A method according to claim 20, wherein for each group of which the party is required to be a member to access the service, the service provider encrypts a different item of data to be provided to said party.

22. A method according to claim 20, wherein the data encrypted in respect of one condition is used as the data to be encrypted in respect of the next condition, the encrypted data resulting from the encryption effected in respect of all said conditions then being provided to the requesting party for decryption in successive decryption operations.

23. A method according to claim 20, wherein the service provider encrypts the data to be provided to said party using public data associated with each of the relevant groups, decryption of the encrypted item only being possible by obtaining a decryption sub-key in respect of each group from the corresponding membership authority.

24. A system for limiting a service to members of a group who are registered with a membership authority, the system comprising:

a first computer entity associated with a provider of said service and arranged to encrypt data based on encryption parameters comprising public data provided by the membership authority and an encryption key string, and to provide the encrypted data to a party;

a second computer entity associated with said party and arranged to decrypt the encrypted data using a decryption key obtained from the membership authority; and

a third computing entity associated with the membership authority and comprising:

- a membership-checking arrangement for checking whether said party is registered with the authority as a member of said group,
- a key-generation arrangement for generating the decryption key in dependence on said encryption key string and private data related to said public data, and
- a control arrangement for enabling the generation of the decryption key by the key-generation arrangement and/or the provision of the decryption key to the second computer entity, only if said party is a group member as checked by the membership-checking arrangement.

25. A system according to claim 24, wherein the encryption key string is created in whole or in part by the first computer entity.

26. A system according to claim 24, wherein the first computer entity is arrange to create, or at least participate in the creation of, said encryption key string upon receipt of a service request from said party, the second computer entity being arranged to receive the encryption key string from the first computer entity and to provide it to said third computer entity to enable the latter to generate and return the decryption key after confirming that said party is a group member.

27. A system according to claim 24, wherein the second computer entity is arranged to create the encryption key string and provide it to the first computer entity when requesting said service, the second computer entity being further arranged to obtain the decryption key from the third computer entity either before or after requesting said service from the first computer entity.

28. A method according to claim 27, wherein the encryption key string is formed using information about at least one of said party and the membership authority, the first computer entity being arranged to use this information in the process of determining whether to provide said service to the party.

29. A system according to claim 24, wherein the third computer entity is arranged to generate the encryption and decryption keys and to provide them to the second computer entity on said party becoming a registered member of said group.

30. A method according to claim 29, wherein the encryption key string is formed using information about at least one of said party and the membership authority, the first computer entity being arranged to use this information in the process of determining whether to provide said service to the party.

31. A system according to claim 24, wherein the data that is encrypted by the first computer entity is a data component of the service, the second computer entity only being able to decrypt and use this data component if said party is a registered member of said group.

32. A system according to claim 31, wherein the data component comprises at least one of software and digital media content.

33. A system according to claim 24, wherein the data that is encrypted by the first computer entity is arbitrary data, the first computer entity being arranged to require the second computer to decrypt and return this data as evidence of its membership of said group before the first computer entity provides said service.

34. A system according to claim 24, wherein in order to obtain the decryption key from the membership authority, the second computer entity is arranged to prove its identity to the third computer entity by using a secret.

35. A system according to claim 34, wherein the second computer entity is a trusted computer platform with secure storage for storing said secret, the third computer entity being arranged to check the integrity of the second computer platform before accepting the proof of identity provided by the latter.

36. A system according to claim 24, wherein the cryptographic processes effected by the first, second and third computer entities in respect of the said encryption and decryption keys are identifier-based cryptographic processes utilising quadratic residuosity.

37. A system according to claim 24, wherein the cryptographic processes effected by the first, second and third computer entities in respect of the said encryption and decryption keys are identifier-based cryptographic processes utilising Weil or Tate pairings.

38. A computing entity comprising:

a first data store for holding private data;

a second data store for holding membership data indicative of members of a group,

a membership-checking arrangement for checking whether a particular party is a member of said group,

a communications interface for receiving an encryption key string from a party requesting the corresponding decryption key, and for outputting the requested decryption key to the requesting party;

a decryption-key generation unit for using the private data and a received encryption key string to generate a corresponding decryption key for decrypting data encrypted using the encryption key string and public data derived using said private data;

a control arrangement for enabling the generation of the decryption key by the decryption-key generation arrangement and/or the provision of the decryption key to a said requesting party via said communications interface, only if that party is a group member as checked by the membership-checking arrangement.